U.S. Department of Commerce
U.S Census Bureau

Privacy Impact Assessment
for the
CEN03, Economic Census and Surveys and Special Processing

Reviewed by: Byron Crenshaw, Bureau Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.09.30 19:17:15 -04'00' 09/21/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
CEN03, Economic Census and Surveys and Special Processing

Unique Project Identifier: 006-000400700

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

CEN03 consists of general support systems and major applications to support Economic statistics and survey collection.

(b) System location

All CEN03 components reside on servers located in Bowie Computer Center (BCC).

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The CEN03 IT system interconnects with internal Census Bureau systems for the purpose of statistical data collection and processing. The CEN03 IT system includes an eCorrespondence project whose goal is to deliver a platform for both incoming and outgoing interactions with customers that can be reused across the Census Bureau by all directorates. It is comprised of a: 1) web application, and 2) PEGA customer relations management (CRM) tool. Each component has a different function, purpose, and interconnection as described below.

Externally, the eCorrespondence portal allows users to have authorized access via the eCorr portal to the Centurion system (CEN15) which stores and manages the survey data. Members of the public accessing Centurion are survey or census respondents. For respondents, the eCorrespondence portal is designed to simplify survey data collection and processing across the enterprise in a cost and time efficient manner.

Internally, the eCorrespondence (eCorr) CRM allows Census Helpdesk Support staff to receive customer inquiries organized into cases and provide resolutions while performing outbound communication based on customer preferences and business rules. The eCorr CRM shares information with the Customer Experience Management (CEM) (CEN05) system about specific cases, which includes CEM customer PII/BII, commitments, events, organizations, contacts, general service requests, data outreach and Frequently Asked Questions (FAQs). Because of the web form component within Pega Customer Relations Management (CRM) system, there is potential internal sharing of encrypted PII, BII or Title 26 if it is included by the respondent within the web form messages.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The Economic Directorate utilizes the IT system for statistical purposes:

The U.S. Census Bureau Economic Programming Directorate is responsible for statistical programs that measure and profile businesses and government organizations in the United States. ECON activities are wide reaching and include: (1) conducting an Economic Census and a Census of Governments every five years; (2) conducting over 50 current surveys taken monthly, quarterly, and annually, including twelve principle economic indicators for the U.S economy; (3) the compilation of administrative records from other government agencies; and (4) facilitating numerous research and technical studies.

The CEN03 IT system has various applications. The applications are designed to accommodate numerous surveys with differing requirements and support all aspects of survey processing. Integrated modules that perform administrative functions allow users to modify the application to meet survey requirements. The surveys process both Title 13 and Title 26 data excluding the construction monthly surveys, which are project based. These applications provide data entry, editing, imputation, data review and correction, estimation and variance estimation. Also, the Census Bureau's master list of businesses called the Business Register (BR). The primary mission of the BR is to provide a complete, unduplicated universe of statistical units that can be used to construct business survey sampling frames and provide a basis for Economic Census enumeration.

The Economic Directorate utilizes the IT system for administrative matters:

The Economic Directorate survey areas use data to create mailing lists of registered businesses. This mailing list designates which individuals receive an authorization code in the mail so that they can submit data for economic-related surveys that are housed in Centurion, which is accessed via the eCorrespondence portal. Use of IRS data allows the ECON directorate to identify the proper individuals who will submit data on behalf of their companies. The eCorrespondence portal collects only enough data to confirm the identity of the individual and create an account for self-service, survey support, and survey collection functionality.

The Economic and Communications Directorate utilize the IT system to improve Federal services online:

The Economic Directorate utilizes the eCorrespondence web application sub-component for approved Census Bureau customers to access survey data. This application performs several survey-related transactions that improve services. For example, users can request a time extension for completing surveys, delegating a survey to another individual, or accessing the Centurion survey data collection system through single sign-on.

For the Communications Directorate, the purpose of the system is to provide the Census Bureau the capability to capture, route, track and respond to every visitor-initiated query that comes through the Census.gov channels. It also allows the Census Bureau to manage its Frequently Asked Questions (FAQ) database and allows website visitors to view and subscribe to receive email notifications when FAQs are updated and can provide real-time customer support by allowing web visitors to submit inquiries via a chat interface.

The Economic Directorate utilizes the IT system for customer satisfaction and online services:

For eCorrespondence, there are two main transaction types in the eCorrespondence system. The first is a respondent self-help transaction. A business respondent logs in and authenticates via a component in the CEN01 security boundary to access the eCorrespondence web application and performs one or more survey-related transactions. This includes requesting delegation of a survey to another individual or accessing the Centurion survey data collection system through single sign-on, etc.

The second type of transaction is a support request. These transactions are managed by the Pega CRM tool. A business respondent can request direct support for a specific survey via secure messaging. Similarly, an anonymous user can submit a message for general support (e.g., for help registering or logging into the website). Support representatives view the submitted secure messages as cases and respond to customers providing interactive support. Only internal Census Bureau staff with a need-to-know may access or view these records.

The goal of the eCorrespondence project is to deliver a platform for both incoming and outgoing interactions with customers that can be reused across the Census Bureau by all directorates. Internally, eCorrespondence Pega will allow Census Helpdesk support staff to receive customer inquiries organized into cases and provide resolutions while performing outbound communication based on customer preferences and business rules. PII/BII is collected to support user account management for survey related transactions. Additionally, the system is also used to document data dissemination activities and to capture interactions with data users. It is also used to track all Census Bureau partnership activities and activities between the Census Bureau and outside organizations.

(e) How information in the system is retrieved by the user

Information (whether personally identifiable information (PII) or business identifiable information (BII)) collected by this IT system are personal names, personal addresses, personal contact information (telephone numbers, email address), business information, occupation, tax information, account information etc. The information is retrieved by PII/BII by Census Bureau staff who have a business need to know. Only Census Bureau employees and their agents with Special Sworn Status can access data under Title 13 U.S.C. Title 13, U.S.C. Section 23 (c) permits the Census Bureau to provide Special Sworn Status to individuals who must access Census Bureau data to assist the Census Bureau in carrying out the work of its title.

(f) How information is transmitted to and from the system

The data is transferred through Electronic Data Transfer (EDT) through the use of: 1) automated rule-based routing and 2) Managed File Transfer (MFT) software components of the system. The EDT system MFT utilizes data integrity checking (hashing) of file content, detection of transfer errors, and recovery from points of failure. The EDT system MFT establishes a secure connection and hashes each packet of data using SHS algorithms. The result(s) of the hashes are transmitted with each packet of data. Encryption is done in-stream, packet by packet, and transmitted to the destination EDT server. Encryption is implemented for data in transit such as SSL/HTTPS to ensure secure transmission of data and web services utilize encrypted security tokens during transmission of data to

prevent access to data outside of an authenticated and valid session and also implemented for data at rest in the databases. Completed data transfers utilize automated rule-based routing (scripting) at destination endpoints for secondary (PIK) processing and quality assurance (QA) against control files.

The eCorrespondence distributes unique, one-time use Authentication Codes mailed to respondents for each survey the respondent participates. When registering or adding a survey to an existing eCorrespondence account, Authentication Codes are verified against data provided by Centurion and eCorresponence associates a survey to a user account in the eCorrespondence database and updates the authentication code bank that the authentication code has been used. Pega CRM provides transactional updates to the eCorr database and queries authentication code status to ensure the code is valid for a specific respondent and associated survey.

(g) Any information sharing conducted by the system

The information in this IT system is shared within the Census Bureau and with other federal agencies such as the Bureau of Justice Statistics, National Center for Education Statistics, Bureau of Transportation Statistics, the Federal Reserve Board, National Science Foundation, U.S. Environmental Protection Agency, Agency for Healthcare Research and Quality, Department of Energy, and the U.S. Department of Housing and Urban Development. In addition, information is shared to the private sector via the Management and Organizational Practices Survey (MOPS) data that is given to the survey sponsors (at Stanford, Massachusetts Institute of Technology, London School of Economics, and the University of Toronto).

Because of the web form component within Pega Customer Relations Management (CRM) system, there is potential internal sharing of encrypted PII, BII or Title 26 if it is included by the respondent within the web form messages. Internally, eCorrespondence (eCorr) CRM allows Census Helpdesk Support staff to receive customer inquiries organized into cases and provide resolutions while performing outbound communication based on customer preferences and business rules.

The eCorr CRM shares information with the Customer Experience Management (CEM) (CEN05) IT system about specific cases, which includes CEM customer PII/BII, commitments, events, organizations, contacts, general service requests, data outreach and Frequently Asked Questions (FAQs).

The data shares include a one way exchange of data from the Micro Analytical Database (MADb) (CEN03) to the Unified Tracking System UTS (CEN05) to support UTS analysis and reporting of survey response rate information for the Company Organization Survey and the Annual Survey of Manufactories (COS/ASM). This data share is internal to survey managers and researchers.

ECON survey paradata is also internally shared with the Master Control System (MCS) (CEN05) and Centurion (CEN15). MCS tracks inputs of survey paradata for data collection and capture and produces outputs of the input data for retrieval by ECON surveys.

ECON also shares read-only public use tabulated data from the Rental Housing Finance Survey (RHFS) with Demographic Statistical Methods Division (DSMD) (CEN11) to create custom tables of organized data access and visualization of RHFS survey data.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

13 U.S.C., Chapter 5, 6, 8(b), 131, 161, 182, 193, and OMB Circular A-133.

For the e-correspondence web application and PEGA CRM system, the following authorities apply: 5 U.S.C. 301 and 44 U.S.C. Section 3101

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Federal Information Processing Standard (FIPS) 199 security impact category for this IT system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.
__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID	X	g. Passport		k. Financial Transaction	X

d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth	X	n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Federal Tax Information such as: Business name, legal form of business, business revenue, number of employees, Business 1040 data, Title 26 Administrative Data, North American Industry Classification System (NAICS).
Health Provider, Health Insurance Coverage, Federal program participation.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	X
Third Party Website or Application			X		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Information accuracy assurance occurs for CEN03 survey systems. The accuracy of the data transferred by EDT is ensured through the use of 1) automated rule-based routing and 2) Managed File Transfer (MFT) software components of the system. The EDT system MFT utilizes data integrity checking (hashing) of file content, detection of transfer errors, and recovery from points of failure.

The EDT system MFT establishes a secure connection and hashes each packet of data using algorithms. The result(s) of the hashes are transmitted with each packet of data and encrypted. Encryption is done in-stream, packet by packet, and transmitted to the destination server. Agorithms are then used to hash the data and compare the result to the hash performed at origination. Both hash results must be equal to ensure that the data has not been compromised in transit. At the end of the file transmission, the connection is closed. Completed data transfers utilize automated rule-based routing (scripting) at destination endpoints for secondary (PIK) processing and quality assurance (QA) against control files.

Within the Business Register, a checksum is performed on every file before and after transfer of data from the system. In addition, analysts are responsible to ensure the data submitted in a given file is accurate. Analysts conduct internal quality assurance processing on all files received from external agencies. Once Analysts conduct QA and approve a file, it is loaded to the Business Register. Additional pre-editing functions are performed to verify validity of specific fields against stored table values, verify data fields are within a specific configured value range, make sure data fields that are dependent on other fields data are configured properly and remove duplicate IDs that are submitted.

eCorrespondence distributes unique, one-time use Authentication Codes mailed to respondents for each survey the respondent participates. Algorithms are implemented within the system to secure authentication codes. When registering or adding a survey to an existing eCorrespondence account, Authentication Codes are verified against data provided by Centurion and eCorresponence associates a survey to a user account in the eCorrespondence database and updates the authentication code bank that the authentication code has been used. Pega CRM provides transactional updates to the eCorr database and queries authentication code status to ensure the code is valid for a specific respondent and associated survey.

Data flagging rules that alert analysts to variances in data that are out of line with expected values, are also implemented to verify that the data that the respondent has entered into the data collection

systems have populated into the processing system correctly. This is usually done by comparing reported data with known information that is received from the IRS or from the same company that is reporting similar or related data to another Census Bureau survey.

Batch edits are also performed to verify data quality and accuracy on a variety of survey specific business rules and flag the workload for survey data analysts in Econ to be able to confirm data corrections, follow up with respondents, look for outliers. Additionally, processing systems automatically alert analysts that there are survey data issues that need to be reviewed both actively (such as receiving a referral listing) or passively (such as an analyst searching for a specific type of data flag for a specific industry via a survey data query tool).

In addition, surveys utilize historic trend analysis and industry trend analysis to alert analysts to potential reporting errors. If dispositions or flags are encountered, survey and system analysts review the potential problems and resolve the issues by generating cases and contacting the respondent to verify the reported values. Analysts are responsible to review data regularly through review and correction modules within Econ processing systems and compare reported values to publicly available data. Testing of the system occurs regularly and whenever a change in the data being collected is implemented.

Custom systems are also utilized to ensure the accuracy of data being reported by respondents by incorporating survey specific flagging rules that alert analysts to variances in data that are out of line with expected values. For example. surveys may use defined parameter edits, respondent correspondence, company website information and comparisons to previous year estimates to check data accuracy as well as edit referrals. Also, those who respond to the survey via Centurion are shown alerts if a data item fails a parameter edit.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. Census has obtained approval from OMB for the collection of survey information per each survey. Individual Paperwork Reduction Act control numbers are assigned to surveys with 10 or more respondents.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For statistical purposes (i.e,, censuses & surveys)			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The Census Bureau will use the PII/BII information collected through the Economic Census and various surveys maintained in CEN03 Economic Census and Surveys and Special Processing IT systems to produce national statistical information.

An example of one of the surveys conducted would be the Annual Capital Expenditures Survey (ACES), which provides broad-based statistics on business spending for new and used structures and equipment.

Another example would be the Annual Retail Trade Survey (ARTS), which uses Business Identifiable Information (BII) to contact the business and obtain the business' financial information.

The information that is collected, processed, and/or maintained within CEN03 components is in reference to members of the public and businesses.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

CEN03 adheres to Census Bureau Data Safeguard, Retention and Acceptable Use Policies that outline the handling of electronic and printed material, proper backup, disposal and recovery of data, user access and data management. Data labeling is in place for systems that handle Federal Tax Information (FTI) and all Census users are also required to take mandated Data Stewardship Awareness Training and Title 26 Awareness Training on an annual basis.

Encryption is implemented for data in transit such as SSL/HTTPS to ensure secure transmission of data and web services utilize encrypted security tokens during transmission of data to prevent access to data outside of an authenticated and valid session. Transparent Data Encryption (TDE) is also implemented for data at rest in the databases.

Consistent system and audit monitoring occurs to validate user and system actions. Suspicious activity is reported to the BOC CIRT within one hour of identification and internal infrastructure and application investigation occurs in parallel with CIRT response investigations to ensure timely remediation.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X*	X**	X
DOC bureaus		X	
Federal agencies	X	X	X
State, local, tribal gov't agencies			
Public			
Private sector			X***
Foreign governments			
Foreign entities			
Other (specify):	* It may be possible the encrypted PII of internal users in the eCorrespondent web/Pega CRM components may be shared internally within the Census Bureau to support and respond to requests.	**Note: Bulk transfer of Title 13 information only from the Business Register.	***Management and Organizational Practices Survey (MOPS) data is shared with the survey sponsors (at Stanford, Massachusetts Institute of Technology, London School of Economics, University of Toronto).

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Unified Tracking IT system (CEN05), Master Control IT system (CEN05), Demographic Surveys and Demographic Statistical Methods Division (CEN11), Center for Economic Studies (CES) (CEN13), and Centurion (CEN15). The CEN03 IT system uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X (eCorrespondence)	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: __https://www.census.gov/about/policies/privacy/privacy-policy.html GovDelivery Privacy Act (PA) https://ask.census.gov/ (for eCorrespondence)	
X	Yes, notice is provided by other means.	Specify how: For eCorrespondence, the mailout letter distributed to survey respondents explains that PII/BII may be collected and maintained for account management purposes. Survey & census introductory letters incorporate Privacy Act Statements
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Various surveys maintained by the CEN03 IT system are voluntary and therefore not required to provide PII/BII. Respondents for voluntary surveys may opt out from creating an eCorrespondence account and submitting survey data. Examples of voluntary surveys are Monthly Wholesale Trade Survey (MWTS), Monthly Retail Trade Survey (MRTS), Monthly Advance Retail Trade Survey (MARTS), and Quarterly Services Survey (QSS).
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: A majority of surveys and the Economic Census are mandatory as required by 13 U.S.C. Individuals are informed of this by one of the following: Privacy Act Statement upon login, letter, interview, or during data collection. Mandatory surveys do not provide an opportunity to decline. All respondents are required to use eCorrespondence and register to respond to surveys.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of

their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: eCorrespondence: Response to some surveys is voluntary and therefore not required to provide PII/BII or consent to particular uses. Examples of voluntary surveys are Monthly Wholesale Trade Survey (MWTS), Monthly Retail Trade Survey (MRTS), Monthly Advance Retail Trade Survey (MARTS), and Quarterly Services Survey (QSS).
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: A majority of surveys and the Economic Census data maintained by the CEN03 IT system are mandatory as required by 13 U.S.C. The data are used for statistical and administrative purposes only and as stated in the Privacy Act Statement provided to respondents. For eCorrespondence, those surveys for which response is not mandatory, there is no opportunity to consent. Respondents are legally obligated to answer all the questions, as accurately as possible.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the Economic Census and surveys maintained by the CEN03 IT system, individuals have the opportunity to provide updates to PII/BII data on the submitted survey or on the survey website. For eCorrespondence, respondents are able to review/update PII/BII pertaining to them via their registration account handled by a component within CEN01
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control *AU-03*, *Content of Audit records*.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 7/6/2020 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Publications are cleared with the Disclosure Review Board.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Oracle Transparent Data Encryption (TDE) for encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

The PII/BII data can only be viewed by a Census federal employee or licensed contractor who has completed up to date training for both Data Stewardship (Title 13) and Title 26. The information can only be accessed on a need to know basis. Employees must use a Census-issued machine (desktop or laptop), or through a secured Virtual Desktop Interface (VDI) session from an approved location for teleworking purposes. Data is stored on local servers, which have been configured to meet all applicable security standards adhered to by the Economic Infrastructure Support (EIS).

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which

information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-4, Economic Survey Collection: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: N1-029-10-2, N1-029-10-3, N1-029-12-004, N1-029-10-4 Company Statistics Division N1-29-10-1 Economic Surveys Division N1-29-03-1NC1-29-80-15, NC1-29-79-4, NC1-29-78-15 NC1-29-78-8 Manufacturing and Construction Division NC1-29-81-10 GRS 3.1: General Technology Management Records; GRS 3.2: Information Systems Security Records; 4.1: Records Management Records; 4.2: Information Access and Protection Records; and GRS 4.3: Input Records, Output Records, and Electronic Copies.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII/BII collected can be directly used to identify individuals.
X	Quantity of PII	Provide explanation: The collection is for Economic Surveys, therefore, a severe or catastrophic number of individuals would be affected if there was loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the act of collecting and using the PII/BII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with organization or mission- specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government- wide or industry-specific requirements. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: PII/BII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned equipment outside of the physical locations, and only with a secured connection.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The Census Bureau is approaching the 2020 Census initiative - survey response online to reduce paper mail outs and collection of the 2020 survey. ECON surveys utilize electronic survey submission of business respondent data currently through systems such as eCorrespondence for the collection of survey data. To ensure respondents are authorized to access and/or submit data related to the survey they are participating in, respondents receive one time use authentication codes that are required to input during account username and password registration. The auth code is linked to the respondents PII/BII and survey they are responding to. In addition, if a respondent forgets their password, respondents must respond to Knowledge Based Verification (KBV) questions to validate they are the person authorized to access the system and data by a specified registered account in accordance with NIST 800-63 Digital Identity Guidelines.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.